UNITED STATES DISTRICT COURT
DISTRICT OF NORTH DAKOTA
EASTERN DIVISION

In re DMS Health Technologies, Inc., Data Breach Litigation	Case No. 3:23-cv-204

DMS HEATH TECHNOLOGIES INC.'S MEMORANDUM IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFF'S CONSOLIDATED COMPLAINT

Defendant, DMS Health Technologies, Inc. ("DMS"), through their respective attorneys of record, submits this Memorandum in support of its Motion to Dismiss Plaintiffs' Stacy Kolkind ("Kolkind") and Constance Boyd's ("Boyd") (sometimes collectively "Plaintiffs") Consolidated Class Action Complaint ("Consolidated Complaint") pursuant to Fed. R. Civ. Pro. 12(b)(6) and Fed. R. Civ. Pro. 12(b)(1).

I. INTRODUCTION

Plaintiffs filed separate class action lawsuits after they received notice of a potential data security event from Defendant, DMS Health Technologies, Inc. ("DMS") that it discovered on April 23, 2023, and that *may* have involved certain of their personally identifiable information ("PII") or personal health information ("PHI") (Dkt. 26). Just like the original pleadings, there is again no allegation (and there will be no evidence) that any information about either Plaintiff or any putative Class Member is in the hands of the criminals or has otherwise been exposed to third-parties as a result of the reported event. Rather, Plaintiffs allege that the unauthorized actor "had the ability to access certain information" and that the criminals had "the intent of engaging in the misuse of PII." (Dkt. 26, ¶¶ 5-6). In this Consolidated Complaint, Plaintiffs attempt to hold DMS liable essentially for doing the right thing: quickly addressing a data security event and notifying any individual who conceivably had a connection to the event even though (as is stated in the

notice), DMS has no reason to believe that any data was exfiltrated or stolen or has been misused in any way after a thorough forensic investigation.

Plaintiffs' Consolidated Complaint is the classic "kitchen sink" pleading that contains eleven counts, four of which are statutory claims under North Dakota, Wisconsin and Minnesota statutes which all address either prohibited disclosure or release of PII or PHI or required notification to individuals when their PII or PHI has been accessed by an unauthorized third-party. The remaining seven counts are a myriad of common law tort and contractual claims and theories of equitable relief. As to the statutory claims, they all fail for three basic reasons: (1) the North Dakota and Minnesota statutes dealing with the unauthorized disclosure of PHI or PII require an active disclosure or affirmative release on the part of a defendant which is not satisfied when the allegation is that a third-party criminal accessed or stole the information in an alleged data breach; (2) the Wisconsin breach notice statute at issue does not provide for a private right of action and does not apply to DMS in this instance; and (3) the final North Dakota "law" Plaintiffs point to does not apply to DMS as it regulation under the Insurance Code of the North Dakota Administrative Code that regulates the insurance industry and North Dakota "licensees."

The common law claims are equally deficient for a number of reasons. Initially, the negligence claim fails to allege a duty. Further, Plaintiffs three contract claims – breach of implied contract, implied covenant of good faith and fair dealing and third-party beneficiary of a contract – all fail as there is no express contact and some of these causes of action either do not exist in the absence of an express contract or are not recognized at all in the relevant states. The invasion of privacy claim is again not clearly recognized in North Dakota and the allegations do not support a claim under other states' laws. The unjust enrichment claim is improper as DMS received no additional benefit for allegedly possessing Plaintiffs' PII. The Declaratory Relief claim fails as

Plaintiffs base this claim on a speculative future data breach. In short, all counts of the Consolidated Complaint should be dismissed pursuant to Fed. R. Civ. P. 12(b)(6) and 12(b)(1).

II. SUMMARY OF PLAINTIFFS' ALLEGATIONS

On March 25, 2024, Plaintiffs filed this Consolidated Complaint on behalf of themselves and purportedly on behalf of a nationwide putative class consisting of all persons "whose PHI was exposed to unauthorized third-parties as a result of the alleged data breach discovered by [DMS] on or around April 23, 2023." (Dkt. 26, ¶ 25). Plaintiff Kolkind, an alleged Texas citizen, additionally purports to bring this matter on behalf of a Wisconsin subclass "whose PHI was exposed to unauthorized third-parties as a result of the event discovered by Defendant on or around April 23, 2023." (*Id*. at ¶ 26). Plaintiff Boyd additionally purports to bring this matter on behalf of a Minnesota subclass "whose PHI was exposed to unauthorized third-parties as a result of the data breach discovered by Defendant on or around April 23, 2023." (*Id*. at ¶ 27.) Plaintiffs' central allegations of wrongdoing against DMS are that it failed to take steps to adequately safeguard their and Class Members' PHI and failed to provide timely and accurate notice to them and other Class Members that their PHI was compromised due to a data breach. (*Id*. at ¶ 42-48).

Plaintiffs allege that they, like Class Members, were required to provide certain PHI to DMS or DMS's clients in order to receive healthcare services. (*Id*. at ¶ 46). They contend that DMS is a North Dakota corporation with its principal place of business in West Fargo, North Dakota. (*Id*. at ¶ 24). They allege that "upon information and belief", unauthorized third-party cyber criminals gained access to Plaintiffs' and Class Members' PHI as "hosted" with DMS and that these cyber criminals acted with intent to misuse their and Class Members' PHI. (*Id.* at ¶ 6). They allege that the "undoubtedly nefarious third party" intends to "profit off this disclosure by defrauding Plaintiffs and Class Members in the future." (*Id.* at ¶ 11). Plaintiffs assert that they and

the putative class members had a reasonable expectation that DMS would implement safeguards to protect their PHI. (*Id*. at ¶ 46).

Boyd, a citizen and resident of Minnesota residing in Hinckley, Minnesota, was a client of Essentia Health Sandstone, a client of DMS. (*Id*. at ¶¶ 23,105). She alleges that in order to obtain medical services from DMS, Boyd was required to provide certain "highly sensitive personal and health information." (*Id.* at ¶ 106). She received notice of the Data Breach via a letter dated October 17, 2023. (*Id*. at ¶ 109). Boyd's allegations surrounding her claimed damages are presented *theoretically* as she alleges that: 1) she was injured by the "material risk to future harm"; 2) that this risk is "imminent and substantial"; 3) that there is a "high risk of identity theft or fraud"; and 4) fraud is likely, "given Defendant's clientele, that some of the Class's information … has already been misused." (*Id*. at ¶ 112). Further Boyd alleges that she has been injured in the form of "lost time dealing with the consequences of the Data Breach," the "diminution in value of her PHI," "increased anxiety" due to the alleged disclosure and "imminent and impending injury" including the "increased risk" of identity theft and fraud. (*Id.* at ¶¶ 111-115). Importantly, Boyd does not allege that she has suffered any out-of-pocket expenses or that the types of injury she fears have actually occurred. (*See, Id.*, generally).

Kolkind, a resident and citizen of Texas residing in Mission, Texas, was a patient of Mayo Clinic in Wisconsin, a client of DMS. (*Id*. at ¶ 17-18). She alleges that she provided her Private Information to Mayo Clinic between March of 2012 and June of 2021. (*Id*. at ¶ 86). Kolkind received notice that her Private Information was potentially exposed via a letter dated September 25, 2023. (*Id*. at. ¶¶ 93, 94). She alleges that a hacker gained access to her email account on or around April 22, 2023. (*Id*. at ¶ 90). Kolkind also contends that "she noticed several unauthorized transactions on her Tremendous prepaid card, totaling at least $190." (*Id*). Kolkind alleges that on

or around April 23, 2023, her "Southwest Airlines voucher (valued at $200), was redeemed for the full amount without her knowledge or permission." (*Id*. at ¶ 91).

Kolkind asserts the following damages occurred as a result of the alleged data breach: 1) an "impending and substantial risk of future harm"; 2) "time and energy spent monitoring her accounts"; 3) "invasion of privacy"; 4) "loss of benefit of the bargain"; 5) "lost time spent on activities remedying harms resulting from the Data Breach"; 6) "lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach"; 7) "diminution of value of her Private Information"; 8) "the continued and increased risk of fraud and identity theft"; 9) "fear, anxiety, and stress" as a result of the Data Breach; and 10) time and money spent monitoring her accounts, including her family's purchase of a $24.99/month credit monitoring service. (*Id*. at ¶¶ 88, 98-103).

Based upon the foregoing, Plaintiffs assert the following causes of action: (1) Negligence; (2) Breach of Implied Contract; (3) Breach of the Implied Covenant of Good Faith and Fair Dealing; (4) Unjust Enrichment; (5) Breach of Contract: Third Party Beneficiary; (6) Invasion of Privacy; (7) Violation of the Wisconsin Notice of Unauthorized Acquisition of Personal Information, Wis. Law. § 134.98, et. seq. (on behalf of Plaintiff Kolkind and the Wisconsin Subclass); (8) Violation of North Dakota's Privacy of Consumer Financial and Health Information, N.D.C.C. § 45-14-01 et. seq; and (10) Violation of the Minnesota Health Records Act, Minn. Stat. §§ 144.291 and 144.293 (on behalf of Plaintiff Boyd and the Minnesota Subclass). Plaintiffs purport to bring all of these causes on their own behalf and on behalf of the putative classes set forth above.

III. MOTION TO DISMISS STANDARD

DMS moves to dismiss the Consolidated Complain under Rule 12(b)(6) for Plaintiffs' "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). To survive a motion to dismiss under Rule 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). While "[t]he plausibility standard is not akin to a 'probability requirement,'" it does require "more than a sheer possibility that a defendant has acted unlawfully" and a complaint that only pleads facts "that are 'merely consistent with' a defendant's liability" will "stop [] short of the line between possibility and probability." *Id*. at 678 (internal citations omitted). Legal conclusions "must be supported by factual allegations" and a Court is "not bound to accept as true a legal conclusion couched as a factual allegation." *Id*. at 678-79 (quoting *Bell Atl.,* 550 U.S. at 555); Finally, "threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." And in "[d]etermining whether a complaint states a plausible claim for relief," the Court is required to "draw on its judicial experience and common sense." *Id*. at 679.

In ruling on a motion to dismiss under Rule 12(b)(6) this Court "may rely on materials 'necessarily embraced by the pleadings,' including exhibits attached to the complaint and matters of public record." *Buckley v. Hennepin Cnty*., 9 F.4th 757, 760 (8th Cir. 2021) (citation omitted); see also *Kuhns*, 868 F.3d 711, 715 (8th Cir. 2017). "[W]hen a written instrument contradicts allegations in the complaint . . . the exhibit trumps the allegations." *Elkharwily v. Mayo Holding Co*., 955 F. Supp. 2d 988, 996 (D. Minn. 2013) (citation omitted). Here, DMS relies only on Plaintiff's pleading and nothing outside the pleading (other than common sense) to attack

Plaintiffs' Consolidated Complaint. Accordingly, all citations to the docket herein are to Plaintiff's Complaint, which is Docket No. 26.

DMS moves to dismiss Count IX for Declaratory Judgement for lack of Article III standing under Rule 12(b)(1). To establish Article III standing, a plaintiff amongst other elements must show an injury in fact. *Quaife v. Brady,* 2024 U.S. Dist. LEXIS 92051 (D. N.D. May 22, 2024). An injury in fact in fact requires "an invasion of legally-protected interest which is (a) concrete and particularized and (b) actual and imminent, not conjectural or hypothetical." *Sierra Club v. Robertson,* 28 F.3d 753, 758 (8th Cir. 1994).

IV. CONFLICTS OF LAW

This Court has very recently held that at the motion to dismiss stage in an alleged data breach class action, the Court should look to the laws of the forum jurisdiction and the states of citizenship of the Plaintiffs and analyze the common-law claims under the laws of all of those states and not perform a full conflicts of law analysis until the discovery stage. *Quaife,* 2024 U.S. Dist. LEXIS 92051. Here, DMS is alleged to be a North Dakota corporation with its principal place of business in North Dakota, Boyd a citizen of Minnesota and Kolkind a citizen of Texas. Oddly, Kolkind seeks to be the representative plaintiff for a Wisconsin subclass consisting of all individuals "within Wisconsin" even though she is neither a Wisconsin resident nor citizen. However, the one Wisconsin statutory claim she asserts is clearly deficient. Accordingly, for purposes of this motion, the common law claims will be analyzed under the laws of North Dakota, Texas and Minnesota pursuant to the *Quaife* Court's very recent instruction.

V. ARGUMENT

All of Plaintiffs' claims have fatal flaws that require dismissal under Fed. R. Civ. Pro. 12(b)(6) for failure to state a claim. DMS addresses Plaintiff's claims in two groups – the various

statutory claims and the common law claims. The four statutory claims fail as the statutes either do no provide for a private right of action, do not apply to DMS or otherwise are not at all applicable to the case at bar. As to the seven common law claims, the contractual claims fail as the none are based on an express contract and DMS took no action that would create an implied contractual obligation. The unjust enrichment claim fails as DMS retained no benefit. The negligence claim fails for lack of duty. Finally, the Declaratory Judgment claim fails as Plaintiffs have not pled an injury in fact sufficient to establish Article III standing. In short, all claims must be dismissed.

A. Kolkind's Count VII Claim for an Alleged Violation of the Wisconsin Notice of Unauthorized Access of Personal Information Act Fails as She is Not a Resident of Wisconsin and There is No Private Right of Action.

Kolkind, a Texas citizen, attempts to assert a claim against DMS, a North Dakota citizen, for an alleged violation of a Wisconsin data breach notification statute – the Wisconsin Notice of Unauthorized Acquisition of Personal Information law ("WNUAPI") Wis. Law. § 134.98 (West 2024). This claim is fatally flawed and must be dismissed for two independently sufficient reasons. First, courts have repeatedly held that there is no private right of action under the WNUAPI. *See, Fox v. Iowa Health System,* 399 F.Supp. 3d 780, 800 (W.D. Wis. 2019); and *In Re Am. Med. Collection Inc. Customer Data Security Breach Litigation,* 2023 U.S. Dist. LEXIS 219588 at *44-45 (D. N.J. 2023). Second, even if any provision of the WNUAPI applies to DMS, Kolkind as a Texas citizen, cannot seek relief from DMS because DMS's principal place of business is not in Wisconsin.

1. There is no private right of action under the WNUAPI.

Case law in the alleged data breach class action context makes clear that there exists no private right of action under the WNUAPI. In *Fox,* the District Court for the Western District of

Wisconsin directly addressed this issue and held that even though a violation of the statute might be used as evidence of negligence, there is no separate private right of action. The Court explained:

> Wisconsin Statute § 134.98 requires companies that do business in Wisconsin to notify their customers within 45 days of a data breach. But the Wisconsin legislature made clear that violation of the statute does not itself establish civil liability . . . .Plaintiffs concede that, under this language, a "bare procedural violation" of the statute does not impose liability or constitute a breach of duty for a negligence claim. But they argue that the legislature intended to impose liability when a defendant's violation of the statute is also a violation of a separate, preexisting duty of care. But that would already be a claim for common law negligence so even in that case, the statute would not create a right of action. Because the legislature has not provided any indication that § 134.98 creates a separate right of action, the court will dismiss plaintiffs' claims under the statute.

Fox, 399 F.Supp. 3d at 800 (citations in original). Likewise, in a 2023 case, the New Jersey District Court relied upon *Fox* and too dismissed a plaintiff's claim under the WNUAPI again holding that there is no private right of action under the statute. *In Re Am. Med. Collection Inc. Customer Data Security Breach Litigation,* 2023 U.S. Dist. LEXIS 219588 at *44-45. Accordingly, Kolkind's Count VII claim for an alleged violation of the WNUAPI must be dismissed as there exists no private right of action.

2. DMS, a North Dakoka citizen, has no responsibility to Kolkind, a Texas citizen, under this Wisconsin Data Breach Notification Statute.

Kolkind alleges to be a Texas citizen and desires to be a class representative for a subclass of "all individuals within Wisconsin" to enforce a Wisconsin data breach notification statute against DMS who she alleges is a "North Dakota corporation with its principal place of business" located in West Fargo, ND. (Dkt. 26, ¶¶ 17, 24). This is contrary to the plain language of the statute. Kolkind alleges that DMS is subject to the WNUAPI because it meets one of the definitions of the term "Entity" under the statute as it "conducts business in the state and maintains personal information in the ordinary course of business." (*Id*. at ¶ 211); Wis. Law. § 134.98(1)(a). Although DMS does not admit it fits that definition of "Entity," for purposes of this Motion, DMS simply

points out that an "Entity" that "conducts business" in Wisconsin, but does not have its principal place of business in Wisconsin or does not license personal information in Wisconsin only is subject to the notice provision of § 134.98(2)(b) which requires such an entity to provide notice of a data breach to Wisconsin residents only.

> **(2) Notice required.**
> **(a)** If an ***entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state*** knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.
>
> **(b)** If an ***entity whose principal place of business is not located in this state*** knows that personal information pertaining to a ***resident of this state*** has been acquired by a person whom the entity has not authorized to acquire the personal information***, the entity shall make reasonable efforts to notify each resident of this state*** who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the ***resident of this state*** who is the subject of the personal information. (Emphasis supplied).

Put simply, section 2(a) of the notice requirement provision applies only to businesses with their principal place of business in Wisconsin or an entity that maintains or licenses information in Wisconsin. DMS is not alleged to be or do either. Accordingly, its only obligation could conceivably be found under 2(b) which requires "entities" whose principal places of business are in a state other than Wisconsin to provide notice to Wisconsin residents. Wis. Law. § 134.98(b). As DMS is a North Dakota citizen and Kolkind is a Texas citizen, this claim must be dismissed.

B. Plaintiffs Count XI Claim for an Alleged Violation of N.D. Cent. Code § 51-22-02 Must be Dismissed as Such a Claim Cannot be Predicated Upon the Alleged "Inaction" of Failure to Secure One's Computer Network.

A very recent decision from this Court made clear that the "disclosure" prohibition in North Dakota Century Code Sec. 51-22-02 ("the ND Non-Disclosure Act") requires some "some type of action" and that the alleged "inaction" of the failure to safeguard personal information from a

cyberattack is not a "disclosure" for purposes of the statute. *Quaife,* 2024 U.S. Dist. LEXIS 92051.

The provision of the ND Non-Disclosure Act at issue provides:

> No business entity which charges a fee for data processing services ***may disclose*** in whole or in part the contents of any record . . . .which is prepared or maintained by such business entity to any person, other then the individual or business entity which is the subject of the record, without the express written consent of such individual or business entity. N.D. Cent. Code § 51-22-02. N.C. Cent. Code § 51-22-02 (Emphasis supplied).

In *Quaife,* the class action plaintiffs alleged a violation of the ND Non-Disclosure Act in a data breach class action where the central allegation of wrongdoing was:

> Defendant disclosed Plaintiffs' and Class Members' PI to third parties without their consent by failing to take appropriate measures to safeguard and protect that PI amidst a foreseeable risk of a cybersecurity attack resulting in the Data Breach. *Id.* at *12-13.

The court reasoned that although the term "disclosure" does not require willfulness or ill-intent, "it does require some sort of action" on the defendant's part and that the allegation of wrongdoing above is based upon alleged "inaction." *Id.* at *12. Accordingly, the Court dismissed plaintiffs' ND Non-Disclosure Act for failure to state a claim stating: "There is no accusation that [Defendant] transferred, published, or distributed the personal information to a third party. The allegations are that cyber criminals accessed [Defendant's] computer system and stole the information." *Id.* at *13.

There is simply no basis to distinguish this case from *Quaife*. In fact, the above-quoted allegation of wrongdoing found in the *Quaife* case is the ***verbatim allegation*** found in Plaintiffs' Complaint in the ND Non-Disclosure Act count in this case:

> Defendant disclosed Plaintiffs and Class Members' PI to third parties without their consent by failing to take appropriate measures to safeguard and protect that PI amidst a foreseeable risk of a cybersecurity attack, resulting in the Data Breach. (Dkt 26, ¶ 242).

As Plaintiffs' allegations are based upon "inaction," they do not amount to disclosure and Plaintiffs' Count Eleven claim under the ND Non-Disclosure Act must be dismissed for failure to state a claim.

C. Similarly, Boyd's Count X Claim for a Violation of the Minnesota Health Records Act Must be Dismissed as DMS Did Not "Release" Her Health Records – Rather She Alleges They Were Stolen by Cybercriminals.

Courts applying Minnesota law have interpreted the prohibitions on unauthorized "release" of a medical record found in Minn. Stat. §§ 144.291 – 144.298 ("the MHRA") in the same manner the *Quaife* Court interpreted the ND Non-Disclosure Act – an entity must commit an "affirmative" release of a record and alleged theft or unauthorized disclosure of a medical records in a data breach is not sufficient. *See, In re Netgain Tech., LLC Consumer Data Breach Litig.,* 2022 U.S. Dist. LEXIS 98342 at *43 (D. Minn. 2022). For example, in *In Re Netgain,* the district court dismissed Plaintiffs' claims under the MHRA where the allegations were exactly the same as in this case – an unauthorized cybercriminal either accessed or exfiltrated and stole medical records during a ransomware attack. *Id.* The court looked to Minnesota Supreme Court precedent which explained the requirement for a "release" under the MHRA and noted that "a person must *affirmatively* release a record that was not authorized for release by the patient's consent." *Id.* at *43 (quoting *Larson v. Nw. Mut. Life Ins. Co.,* 855. N.W. 2d 293, 302 (Minn. 2014)). Accordingly the court held that a cybercriminal's alleged act of exfiltrating and stealing information during a data breach does not amount to a "release" by the defendant. The court explained:

> Netgain never affirmatively released the health records to the cybercriminals. Instead, as is alleged in the Amended Complaint, the cybercriminals exfiltrated (i.e. stole) Plaintiffs' sensitive information. And stealing does not constitute an affirmative release as required by the statute. *Id.*

The rationale of *In re Netgain* is solid and comports to the language of the statute as well as the rationale applied by this Court in *Quiafe* in its discussion of the ND Non-Disclosure Act. Accordingly, dismissal of Count X is proper pursuant to Rule 12(b)(6).

D. Plaintiffs' Count VIII Claim Purportedly for a Violation of North Dakota's Privacy of Consumer Financial Health Information Law is Completely Off-Base and Must be Dismissed.

This Count seems to be asserted in error as N.D. Cent Code Sec. 45-14-01 is entitled "Nature of Partnership" and has nothing to do with consumer and financial health information. *See, N.D. Cent. Code §* 45-14-01 et. seq. Further, many of the sections have been repealed. DMS assumes that Plaintiffs may be referring to Section 45 of the North Dakota Administrative Code that regulates the insurance industry ("Insurance Code") in North Dakota as Plaintiffs allege that DMS violated § 45-01-14-17 "when it disclosed Plaintiffs' and Class Members' nonpublic health information without their authorization." (Dkt. 26, ¶ 219). However, Sec. 45-01-14-17 applies only to a "licensee" as that term is defined in the Insurance Code. Section 45-01-14-04(17.a.) defines a licensee under the Insurance Code as:

> 17. a. "Licensee" means all licensed insurers, producers, and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the insurance law of this state and health maintenance organizations holding a certificate of authority pursuant to North Dakota Century Code chapter 26.1-18.1.

DMS is not alleged to be, and is clearly not, a licensee under the Insurance Code. Accordingly, Count VIII must be dismissed with prejudice pursuant to Rule 12(b)(6).

E. Plaintiffs Fail to Allege Any Conduct on the Part of DMS That Gives Rise to a Claim for Breach of Implied Contract.

To state a claim for breach of an implied contract, a plaintiff must plead the existence of a valid implied contract, performance or tendered performance by the plaintiff, breach of the implied contract by the defendant, and damages resulting from the breach." *Electrostim Med. Servs., Inc.*

v. Health Care Serv. Corp., 614 F. App'x 731, 744 (5th Cir. 2015). In all relevant jurisdictions, the elements of breach of contract are the same for express or implied, but the question of whether a contract exists in the implied contract setting is based upon the objective manifestations of the parties through words and actions. *Id.* (Texas Law); *Hall,* 2023 U.S. Dist. LEXIS at *14 (D. Minn.) (Minnesota law); *Lord & Stevens, Inc. v. 3D Printing, Inc.,* 2008 ND 189, 756 N.W.2d 789, 792 (N.D. 2008).

Here, Plaintiffs point to no objective conduct by DMS evidencing a contractual promise to secure their data. In fact, it is unclear if Plaintiffs even had any knowledge at all that they had any connection to DMS as they both allege that the received medical services at health care facilities that are customers or clients of DMS. Further, both Plaintiffs allege that they tendered their information to other parties – the Mayo Clinic and Essentia Health Sandston. (Dkt., 26, ¶¶ 20, 105). At a minimum, Plaintiffs must plead what words, actions or other manifestations DMS made (and not those of the Mayo Client or Essentia Healthcare Sandstone) that would lead Plaintiff to believe they had a contract with DMS that included data security provisions. *See, e.g.*, *SuperValu II*, 870 F.3d at 771 n.6 (finding plaintiffs did not become parties to an implied contract to protect PII simply by giving defendant their payment information); *SuperValu IV*, 925 F.3d at 965-966; *Cmty. Bank of Trenton*, No. 15-cv- 01125-MJR, 2017 WL 1551330, at *5 (S.D. Ill. May 1, 2017) (finding "implicit promise" of data security insufficient to support implied contract claim), *aff'd*, 887 F.3d 803 (7th Cir. 2018). Accordingly, Plaintiffs have failed to properly plead facts to establish the existence of an implied contract claim and the Count II claim must be dismissed.

F. Plaintiffs Cannot State a Claim for Breach of Implied Covenant of Good Faith as the Claim is Either Not Recognized and Very Narrow and Cannot Exist in the Absence of an Express Contract.

Although there is some minor variance in the laws of North Dakota, Texas and Minnesota as to this claim, it is clear that under all of these state's jurisprudence, dismissal is required because Plaintiff does not even plead the existence of an express contract, but rather a generic implied contract. Initially, North Dakota flatly rejects such a claim as North Dakota courts and courts applying North Dakota Law have repeatedly held that the cause of action does not exist outside of the insurance contract setting. *See, e.g.,* W*FND, LLC v. Fargo Marc, LLC*, 2007 ND 67, 730 N.W.2d 841, 851 (N.D. 2007); *Pitchblack Oil, LLC v. Hess Bakken Invs. II, LLC*, 949 F.3d 424, 428 (8th Cir. 2020). Specifically, the North Dakota Supreme Court has repeatedly held that such a claim cannot survive even when there is a concrete written contract and that the *only* exception to this general rule is for insurance contracts. *Id., See also, Barnes V. St. Joseph's Hospital,* 1999 ND 204, 601 N.W.2d 587 (N.D. 1999). The North Dakota Supreme Court explained:

> In North Dakota, the doctrine of an implied covenant of good faith and fair dealing has only been applied to insurance contracts. Moreover, the implied covenant of good faith and fair dealing . . . . does not operate to alter the material terms of a contract. . .. nor does the duty of good faith inject substantive terms into the parties' contract.

WFND, LLC, 730 N.W.2d at 851; *See also, Pitchblack Oil,* 949 F.3d at 428 ("North Dakota does not apply the implied covenant of good faith and fair dealing to any contract other than an insurance agreement").

Texas courts also recognize that the cause of action is extremely limited *Indep. Fin. Grp., LLC v. Quest Trust Co.*, U.S. Dist. LEXIS 236718 (S.D. Tx. 2022). Specifically, "not all contracts contain an implied covenant of good faith and fair dealing." *Houle v. Casillas* 594 S.W.3d 524 (Tex. App.—El Paso 2019, no pet) citing *Saucedo v. Horner*, 329 S.W.3d 825, 831-32 (Tex. 2010)). The claim "is a tort action that arises from an underlying contract." *Saucedo*, 329 S.W.3d at 831.

Texas differs from other states in that "contracting parties owe a good-faith duty only if they expressly agree to act in good faith, a statute imposes the duty, or the parties have a 'special relationship' like that between an insurer and insured." *Dallas/Fort Worth Int'l Airport Bd. v. Vizant Techs., LLC*, 576 S.W.3d 362, 369 n.13 (Tex. 2019) (citing *Subaru of Am. v. David McDavid Nissan, Inc.*, 84 S.W.3d 212, 225 (Tex. 2002)). Only in cases where there is a special relationship, such as between an insurer and its insured, does Texas law impose an actionable duty of good faith and fair dealing. *Id.* Whether the duty exists is a question of law. *Id.*

Finally, under Minnesota law, although every contract includes an implied covenant of good faith and fair dealing, the doctrine is applied to ensure that one party not "unjustifiably hinder" the other party's performance of a specific contractual obligation. *In re Hennepin Cnty. 1986 Recycling Bond Litigation*, 540 N.W.2d 494, 502 (Minn. 1995); *Churlik Gate City Bank*, 2024 U.S. Dist. LEXIS 20090 (Dist. Minn. 2024). Accordingly, a party acts in bad faith if it refuses "to fulfill some duty or contractual obligation based on an ulterior motive." *Kivel v. WealthSpring Mortg. Corp.*, 398 F.Supp.2d 1049, 1057 (D. Minn. 2005). Moreover, merely seeking to maximize profits is insufficient to show bad faith. *BP Prods. N. Am., Inc. v Twin Cities Stores*, 534 F. Supp. 2d 959, 967 (D. Minn. 2007).

Here, Plaintiffs do not even allege the existence of an express contract, but rather an implied contract based upon alleged actions of DMS. So, Plaintiffs' claim is for breach of an implied covenant of good faith and fair dealing included in an alleged implied contract. Obviously, if the North Dakota Supreme Court does not inject an implied covenant of good faith and fair dealing into express written or oral contracts it certainly would not inject such an implied covenant into an alleged implied contract with no defined terms. Further, under Texas law there is certainly no preexisting "special relationship" like the insurer-insured that would lead to the legal creation

of such a claim in the absence of even an actual express contract. Finally, and relevant to Minnesota law, there is no allegation that DMS has an ulterior motive in itself being the victim of a data security event or that it tried to hinder Plaintiffs from performing a contractual obligation. After all, Plaintiffs claim their only obligation was to tender PHI or PII. In short, the claim for Breach of Implied Covenant of Good Faith and Fair Dealing is flawed under all relevant state laws and must be dismissed with prejudice pursuant to Fed. R. Civ. P Rule 12(b)(6).

G. Plaintiffs Have Not Stated a Claim for Unjust Enrichment as They Do Not Allege That DMS Failed to Provide the "Services" She Sought or That DMS Was Paid Extra for "Data Protection."

Unjust enrichment is an equitable doctrine which rests upon contract or quasi-contract theories of recovery and a benefit conferred by one party at the unjust expense of another. As the North Dakota Supreme Court succinctly stated, "the essential element in recovering under the theory of is the receipt of a benefit by the defendant from the plaintiff which would be inequitable to retain without paying for its value." *McDougal v. AgCoutnry Farm Credit Servs, PCA,* 937 N.W.2d 546, 553 (N.D. 2020). Minnesota and Texas courts apply the same standards. *See e.g., Hall v. Centerspace, LP,* 2023 Dist. LEXIS 83438 (D. Minn. 2023); and *Heldenfels Bors., Inc. v. City of Corpus Christi,* 832 S.W.2d 39, 41 (Tex. 1992).

In *Quaife,* this Court rejected an unjust enrichment claim in the data breach context under both North Dakota and Minnesota law because there can be no unjust enrichment if the plaintiff does not allege to have received the benefit of the bargain – i.e. the services at issue. *Quaife,* 2024 U.S. Dist. LEXIS 92051 at * 11 -12. Likewise, a recent case from the District of Minnesota held the plaintiffs could not state an unjust enrichment claim in the data breach context because there was no indication that plaintiffs paid more to "secure data security than those who did not provide PII." *Hall,* 2023 Dist. LEXIS 83438 at *21 – 22. Finally, the Eight Circuit Court's opinion in

Alleruzzo v. SuperValu, Inc. 925 F.3d 955 (8th Cir. 2019), although it applied Illinois state law to an Unjust Enrichment claim, is instructive. *Id.* at 966. The plaintiff alleged that the defendant supermarket paid for groceries with a credit card and that her information was later obtained by the hackers. Plaintiff alleges that had she known of a data breach, she would not have shopped at defendant's store. *Id.* The Court rejected Plaintiff's argument and dismissed the unjust enrichment claim, holding that Plaintiff concedes she received her groceries and did not pay a premium for data security. The court explained:

> Common sense counsels against the viability of [plaintiff's] theory of unjust enrichment. Holmes paid for groceries. The price would have been the same whether he paid with cash or a credit card. He did not pay a premium for a 'side order of data protection'. *Id.*

The exact same logic applies. Plaintiffs claim to have tendered personal information in order to receive DMS's undefined "services." Plaintiffs do not allege that DMS failed to provide those services or that DMS charged them extra to safeguard her personal information or that the services would have cost less if lesser security measures were provided. Instead, Plaintiffs ambiguously allege that they "did not receive the benefit of their bargain because they paid for health care products/and or health care services that did not satisfy the purposes for which they bought them." (Dkt., 26, ¶ 179). This is simply not what the doctrine of Unjust Enrichment addresses. Accordingly, Count IV for unjust enrichment must be dismissed with prejudice under Rule 12(b)(6).

H. Plaintiff's Cannot State a Claim for Breach of Contract on a Third-Party Beneficiary Theory for a Number of Reasons.

A third party may recover on a contract made between other parties only if the parties intended to secure a benefit to that third party, and only if the contracting parties entered into the contract directly for the third party's benefit. *MCI Telecomms. Corp. v. Texas Util. Elec. Co.*, 995 S.W.2d 647, 651 (Tex. 1999). A third party does not have a right to enforce the contract if she

received only an incidental benefit. *Id.* "A court will not create a third-party beneficiary by implication." *Id.* Rather, an agreement must clearly and fully express an intent to confer a direct benefit to the third party. *Id.* Further, "it must appear by express stipulation or by reasonable inference that that the rights and interests of such unnamed parties were contemplated and provision was made for them." *McShane Construction Co., LLC v. Gotham Ins. Co.,* 867 F. 3d 923, 930 (8th Cir. 2017). Minnesota has adopted the "intended beneficiary approach" wherein there must be an express duty owed to the third-party in the contract or that the beneficiary is the intended beneficiary of the promised performance. *Hickman v. Safeco Ins. Co. of America,* 695 N.W.2d 365, 369 (Minn. 2005). Again, merely being an "incidental beneficiary" of a contract is not enough. *Id.*

Here, Plaintiffs fall woefully short of establishing they have a right to enforce any contract between DMS and some unnamed "clients" of DMS. To wit, Plaintiffs vaguely allege that "[DMS] and [DMSs' clients] contracted for imaging services" and that "upon information and belief" these contracts included promises to "provide data retention and security services" and comply with laws and industry standards. (Dkt. 26, ¶¶ 187 – 188). DMS is left to assume that Plaintiffs are alleging the existence of contracts between DMS and the Mayo Clinic (Kolkind) and DMS and Essentia Health Sandstone (Boyd). Even if such contracts exist, there can be no way to determine from Plaintiffs' allegations that they were the intended beneficiaries of this contract. The intended beneficiaries would be the contracting parties. This is not a will or trust agreement where the ***intent*** of the contract is to benefit a third-party. After all, DMS had no idea who Plaintiffs were. Rather, assuming *arguendo*, there are data security provisions in these hypothetical contracts with unnamed clients, Plaintiffs would be, at best, incidental beneficiaries of those provisions. This is

not enough. Accordingly, Count V must be dismissed with prejudice pursuant to Fed. R. Civ. Pro. 12(b)(6).

I. Plaintiffs' Claim for Invasion of Privacy Must be Dismissed as Plaintiffs Voluntarily Tendered Their Information and They Allege That it Was a Third-Party Criminal That Tried to Steal Their Information – Not DMS.

Although not specifically labeled as such, Plaintiffs Count VI claim for Invasion of Privacy is based upon an intrusion upon seclusion theory as they allege that the "unauthorized release" of their PHI or PII was "highly offensive" and that this "intrusion was into a place or thing." (Dkt. 26, ¶¶ 201 – 202). In North Dakota, it is unclear if the tort of invasion of privacy based upon an intrusion upon seclusion even exists. *Hogum v. Valley Memorial Homes,* 574 N.W.2d 812, 818 (N.D. 1998). In Minnesota, intrusion upon seclusion is when someone "intentionally intrudes, physically or otherwise, upon the solitude of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person. *Lake v. Walmart Stores, Inc.* 582 N.W.2d 231, 233 (Minn. 1998); *In re Group Health Plan Litigation,* 2023 U.S. Dist. LEXIS (D. Minn 2023). In Texas, "Usually an action for intrusion upon one's seclusion is found only when there has been a physical invasion of a person's property or ... eavesdropping on another's conversation with the aid of wiretaps, microphones, or spying." *Graham v. JPMorgan Case Bank, Nat. Ass'n*, 2015 U.S. Dist. LEXIS 93045, (S.D. Tex. July 15, 2015) (quoting *Ross v. Midwest Commc'ns, Inc.*, 870 F.2d 271, 273 (5th Cir. 1989)).

Here, there can be no claim for intrusion upon seclusion because DMS did not "intrude" upon Plaintiffs in anyway. Rather, as Plaintiff clearly alleges, they willfully gave their PII or PHI to DMS or DMS's client and it was allegedly stolen or criminally accessed by an unknown third-party criminal. So, if anyone "intruded" upon Plaintiffs' seclusion, it was the criminal and not DMS. A federal district court in Wisconsin recently addressed this claim and succinctly addressed

the issue. *Linman v. Marten Transp.,* 2023 U.S. Dist. LEXIS 45661 (W.D. Wis. 2023) (applying Wisconsin law). In *Linman,* the Court, applying Wisconsin law in an alleged data breach class action extremely similar to the case at bar, explained how an Invasion of Privacy – Intrusion Upon Seclusion claim cannot exist under Wisconsin law because the plaintiff admits it voluntarily gave its PII to the defendant and that it was a third-party and not the defendant who was alleged to have improperly stolen it. *Id.* at *12. The court explained:

> Linman hasn't stated a claim for intrusion upon seclusion for one simple reason: ***it was the hackers, not Marten, that intruded on Linman's privacy***. Linman provided his personal information to Marten willingly, so it didn't intrude on his privacy by collecting it. The only "intrusion" was the alleged breach by the hackers. (Emphasis supplied).

Id.; *See also, In re Group Health Plan Litigation,* 2023 U.S. Dist. LEXIS (D. Minn 2023) (court found plaintiff plausibly stated intrusion upon seclusion claim under Minnesota law where it installed tracking pixel software on its website and collected plaintiff data without its consent and voluntarily shared it with third-parties for marketing and data analytic purposes).

Here, Plaintiffs do not allege that DMS unlawfully obtained their PII or PHI. Rather, they allege they voluntarily tendered in the information. Plaintiffs do not allege that DMS voluntarily shared their information with a third-party. Rather, they allege DMS was itself a victim of a cyberattack wherein criminals attempted to steal the information. Given these facts, this Court should follow the logic of *Linman* and dismiss with prejudice Plaintiffs' claim for invasion of privacy.

J. The Negligence Claim Fails as Plaintiff's Allegations to Establish a Legal Duty are Insufficient and Vague.

DMS acknowledges that this Court recently recognized the possibility that a defendant may owe a duty "at least at this early stage" of litigation to have sufficient data security measures because a data breach may be foreseeable. *Quaife,* 2024 U.S. Dist. LEXIS 92051 at *8. However,

this Court also recognized that such a duty must be established through "sufficient factual allegations" as to both foreseeability, the entrustment of data and a connection with the personal information stolen. Here, Plaintiffs' allegations of the nature of the relationship between themselves and DMS are contradictory and vary from paragraph to paragraph. For example, Plaintiffs plead generally that they tendered their PII or PHI to the Mayo Clinic (Kolkind) or Essentia Health Sandstone (Boyd). But in other counts, and particularly the Unjust Enrichment Count, they allege a duty and special relationship created by the fact that they tendered their information to DMS. For example, they allege they would not have tendered their PII to DHS "had they known [DMS's] systems were substandard" for data protection purposes. (Dkt. 26, ¶ 175). In short, Plaintiffs cannot have it both ways.

DMS is not necessarily saying that Plaintiffs may not potentially be able to allege a duty, but they have not in the Consolidated Complaint. DMS understands that Plaintiffs can plead claims in the alternative, but they cannot plead facts in the alternative. In short, Plaintiffs' contradictory and vague allegations call into question the nature and scope of any duty owed by DMS to Plaintiffs and the negligence claim must be dismissed.

K. The Declaratory Judgment Count Must be Dismissed for Lack of Standing 12(b)(1).

Based upon Plaintiffs' allegations and the alleged risk of future harm, they lack standing to assert the claim for Declaratory Judgment under Fed. R. Civ. Pro. 12(b)(1). *See, Hall,* 2023 U.S. Dist. LEXIS at & 7 – 13. Here, Plaintiffs' claim for Declaratory Judgement is predicated solely on the hypothetical instance that DMS suffers a future data security event and the further hypotheticals that their information is impacted and that DMS did nothing to enhance security practices. (Dkt. 26, ¶¶ 224 – 228). The Court in *Hall* addressed this very theory and concluded that in a data breach case like this, in order to establish standing and show that the hypothetical future harm is

"sufficiently imminent" there must be specific facts pled to "indicate that a second data breach is certainly impending, or even that there is a substantial risk that one will occur." *Id.* at *10.

DMS acknowledges that this Court in *Quaife* that there were sufficient allegations to establish standing since the plaintiff had alleged a "risk of harm and injury in fact as to the stolen personal information." *Quaife,* 2004 U.S. Dist. LEXIS at *14. However, here and like as in *Hall,* the Declaratory Judgement action is not based upon information that was allegedly already subject to access. Rather, is relates solely to the alleged possibility of a future a data breach. There is simply no allegation that there is somehow another data breach on the horizon. After all, any company in the world could be subject to a data breach. But that speculative possibility is not enough for Article III standing. Accordingly, the Count IX claim for Declaratory Judgement should be dismissed pursuant to Fed. R. Civ. Pro. 12(b)(1).

VI. CONCLUSION

Based upon the arguments and authorities contained herein, Defendant DMS Health Technologies Inc., respectfully requests that this Honorable Court dismiss all counts of Plaintiffs' Consolidated Complaint with prejudice pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6).

Respectfully submitted:

O'HAGAN MEYER LLC

/s/ James W. Davidson
James W. Davidson, Admitted *Pro Hac Vice*
O'Hagan Meyer LLC
One East Wacker Drive, Suite 3400
Chicago, Illinois 60601
(312) 422.6100 – T
jdavidson@ohaganmeyer.com
Attorney for Defendant, DMS Health Technologies, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on May 31, 2024, all counsel of record who are deemed to have consented to electronic service are being served a true and correct copy of the foregoing document using the Court's CM/ECF system:

Todd Michael Miller
Solberg Stewart Miller
PO Box 1897
Fargo, ND 58107-1897
701-237-3166
tmiller@solberglaw.com

MIGLIACCIO & RATHOD LLP
Nicholas A. Migliaccio, Admitted *Pro Hac Vice*
412 H Street N.E., Suite 302
Washington, D.C. 20002
T: (202) 470-3520
nmigliaccio@classlawdc.com

/s/ James W. Davidson
James W. Davidson, IL ARDC No. 6281542
O'Hagan Meyer LLC
One East Wacker Drive, Suite 3400
Chicago, Illinois 60601
312.422.6100 –T
312.422.6110 – F
jdavidson@ohaganmeyer.com